氏名（本籍）	程　民権（中　国）
学位の種類	博　士（工　学）
学位記番号	博甲第6053号
学位授与年月日	平成24年3月23日
学位授与の要件	学位規則第4条第1項該当
審査研究科	システム情報工学研究科
学位論文題目	**Anti-Collusion Codes and Tracing Algorithms for Multimedia Fingerprinting** （マルチメディア指紋におけるアンチ結託符号および追跡アルゴリズム）

主査	筑波大学教授	工学博士	山本芳嗣
副査	筑波大学准教授	博士（理学）	繆　瑩
副査	筑波大学教授	Ph.D. in Combinatorics and Optimization	藤原良叔
副査	筑波大学教授	博士（工学）	張　勇兵
副査	筑波大学准教授	博士（学術）	八森正泰
副査	筑波大学准教授	博士（工学）	古賀弘樹

論文の内容の要旨

本論文のテーマは、電子データの不法な再配布を抑止するため、線形結託攻撃に対処できる新たな電子指紋用のコードと、それを用いた結託者の追跡アルゴリズムの開発である。

第1章で電子データの不法な再配布が近年問題になっていることを指摘し、第2章で電子指紋のこれまでの研究成果を概観している。結託した複数の利用者が彼らの電子指紋を線形的に重ね合わせることによって身元を隠す線形結託攻撃を紹介し、この種の攻撃に対して結託者を追跡するための既存のアルゴリズムを紹介している。扱うべき問題も結託者追跡アルゴリズムも、送信された元の電子データを追跡者が入手可能かどうかで大きく変わるが、この論文では元のデータが入手可能との状況（non blind）を考えることが断られている。

第3章の前半では、既存のAND-ACC（AND anti-collusion code）をseparable matrixによって特徴づけており、これによってseparable matrixを構成することによってAND-ACCを構成できることを示している。さらに、既存の追跡アルゴリズムの1つであるhard detection algorithmの欠陥を指摘し、改良アルゴリズムを提案している。このアルゴリズムの計算複雑度は利用可能者人数Mと電子指紋の次元nの積Mnの線形オーダーであり、従来のアルゴリズムより大きく改善されている。第3章の後半では、新しくLACC（logical anti-collusion code）を提案している。AND-ACCはサイズがパラメータt以下のコードの部分集合に対するビット毎のAND演算結果に条件を課して定義されているが、提案されたコードLACCはさらにOR演算結果も考慮したものである。この結果、これまで結託者追跡に不向きとされていたFPC（frameproof code）についても追跡性能があることが指摘されている。

第4章はSC（separable code）の構成とその利用可能者人数Mの上界値の計算がテーマである。既知の複数のSCを組合せて新しいSCを構成する方法を提案し、射影平面や巡回差行列に基づきn=2と3のときの最適なSCの構成法も示している。さらに、Mの上界値の計算のため、SCの構造上の特徴から導かれる非

線形制約を持つ整数最適化問題が考慮され、その最適解での目的関数値が良い上界を与えることが述べられている。この最適化問題の整数条件を緩めた連続緩和問題の最適値の計算によりMの上界を与えている。さらに、整数条件を考慮したまま最適解の範囲をどのように狭めることができるか議論して、新しい上界を提案している。

第5章では確率的追跡アルゴリズムを提案している。LACCを使った場合、パラメータtが実際に結託した人数以上の場合には結託者を追跡できるが、そうでない場合には追跡できない。しかし、実際の場面では当然結託者人数を知ることはできないので、この性質は大きな欠点である。この欠点を克服するため、マルコフ連鎖モンテカルロ法に基づいた確率的追跡アルゴリズムを提案し、シミュレーションによってその性能を確かめている。

審 査 の 結 果 の 要 旨

LACC（logical anti-collusion code）の提案、SC（separable code）の構成とその利用可能者人数Mの新しい上界値の計算、確率的追跡アルゴリズムの提案など、この分野への貢献は大きい。論文には推敲すべき余地が若干残されているが、十分博士論文の水準に達している。

平成24年2月8日、システム情報工学研究科において、学位論文審査委員の全員出席のもと、著者に論文について説明を求め、関連事項につき質疑応答を行った。その結果、学位論文審査委員全員によって、合格と判定された。

上記の学位論文審査ならびに最終試験の結果に基づき、著者は博士（工学）の学位を受けるに十分な資格を有するものと認める。